The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
8/29/2012

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Firefox versions prior to 15
Firefox Extended Support Release (ESR) versions prior to 10.0.7
Thunderbird versions prior to 15
Thunderbird Extended Support Release (ESR) versions prior to 10.0.7
SeaMonkey versions prior to 2.12

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

Miscellaneous memory safety hazards (MFSA 2012-57)

Several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products have been identified. Some of these bugs showed evidence of memory corruption under certain circumstances, and some of these could be exploited to run arbitrary code.

Multiple Use-after-free issues (MFSA 2012-58)
Multiple use-after-free issues have been discovered. Many of these issues are potentially exploitable, allowing for remote code execution.

Location object can be shadowed using Object.defineProperty (MFSA 2012-59)
It is possible to shadow the location object using Object.defineProperty. This could be used to confuse the current location to plugins, allowing for possible cross-site scripting (XSS) attacks.

Escalation of privilege through about:newtab (MFSA 2012-60)
When a page opens a new tab, a subsequent window can then be opened that can be navigated to about:newtab, a chrome privileged page. Once about:newtab is loaded, the special context can potentially be used to escalate privilege, allowing for arbitrary code execution on the local system in a maliciously crafted attack.

Memory corruption with bitmap format images with negative height (MFSA 2012-61)
Two related issues with the decoding of bitmap (.BMP) format images embedded in icon (.ICO) format files have been discovered. When processing a negative "height" header value for the bitmap image, a memory corruption can be induced, allowing an attacker to write random memory and cause a crash. This crash may be potentially exploitable.

WebGL use-after-free and memory corruption (MFSA 2012-62)
Two WebGL issues have been discovered. The first issue is a use-after-free when WebGLshaders are called after being destroyed. The second issue exposes a problem with Mesa drivers on Linux, leading to a potentially exploitable crash.

SVG buffer overflow and use-after-free issues (MFSA 2012-63)
Two issues involving Scalable Vector Graphics (SVG) files have been identified. The first issue is a buffer overflow in Gecko's SVG filter code when the sum of two values is too large to be stored as a signed 32-bit integer, causing the function to write past the end of an array. The second issue is a use-after-free when an element with a "requiredFeatures" attribute is moved between documents. In that situation, the internal representation of the "requiredFeatures" value could be freed prematurely. Both issues are potentially exploitable.

Graphite 2 memory corruption (MFSA 2012-64)
Two memory corruption issues involving the Graphite 2 library used in Mozilla products have been discovered. Both of these issues can cause a potentially exploitable crash. These problems were fixed in the Graphite 2 library, which has been updated for Mozilla products.

Out-of-bounds read in format-number in XSLT (MFSA 2012-65)

An out-of-bounds read in the format-number feature of XSLT has been discovered. This can cause inaccurate formatting of numbers and information leakage. This is not directly exploitable.

HTTPMonitor extension allows for remote debugging without explicit activation (MFSA 2012-66)
An issue with the Firefox developer tools' debugger has been identified. If remote debugging is disabled, but the experimental HTTPMonitor extension has been installed and enabled, a remote user can connect to and use the remote debugging service through the port used by HTTPMonitor. A remote-enabled flag has been added to resolve this problem and closes the port unless debugging is explicitly enabled.

Installer will launch incorrect executable following new installation (MFSA 2012-67)
If a crafted executable is placed in the root partition on a Windows file system, the Firefox and Thunderbird installer will launch this program after a standard installation instead of Firefox or Thunderbird, running this program with the user's privileges.

DOMParser loads linked resources in extensions when parsing text/html (MFSA 2012-68)
When the DOMParser is used to parse text/html data in a Firefox extension, linked resources within this HTML data will be loaded. If the data being parsed in the extension is untrusted, it could lead to information leakage and can potentially be combined with other attacks to become exploitable.

Incorrect site SSL certificate data display (MFSA 2012-69)
Incorrect SSL certificate information can be displayed on the address bar, showing the SSL data for a previous site while another has been loaded. This is caused by two onLocationChange events being fired out of the expected order, leading to the displayed certificate data to not be updated. This can be used for phishing attacks by allowing the user to input form or other data on a newer, attacking, site while the credentials of an older site appear on the address bar.

Location object security checks bypassed by chrome code (MFSA 2012-70)
Certain security checks in the location object can be bypassed if chrome code is called content in a specific manner. This allowed for the loading of restricted content. This can be combined with other issues to become potentially exploitable.

Insecure use of __android_log_print (MFSA 2012-71)
A vulnerability affecting Mozilla Firefox for Android devices has been discovered. The function __android_log_print is called insecurely in places. If a malicious web page used a dump() statement with a specially crafted string, it can trigger a potentially exploitable crash.

Web console eval capable of executing chrome-privileged code (MFSA 2012-72)
The eval command in the web console can execute injected code with chrome privileges, leading to the running of malicious code in a privileged context. This allows for arbitrary code execution through a malicious web page if the web console is invoked by the user.
Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade vulnerable Mozilla products immediately after appropriate testing.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Do not open email attachments or click on URLs from unknown or untrusted sources.

Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/
http://www.mozilla.org/security/announce/2012/mfsa2012-57.html
http://www.mozilla.org/security/announce/2012/mfsa2012-58.html
http://www.mozilla.org/security/announce/2012/mfsa2012-59.html
http://www.mozilla.org/security/announce/2012/mfsa2012-60.html
http://www.mozilla.org/security/announce/2012/mfsa2012-61.html
http://www.mozilla.org/security/announce/2012/mfsa2012-62.html
http://www.mozilla.org/security/announce/2012/mfsa2012-63.html
http://www.mozilla.org/security/announce/2012/mfsa2012-64.html
http://www.mozilla.org/security/announce/2012/mfsa2012-65.html
http://www.mozilla.org/security/announce/2012/mfsa2012-66.html
http://www.mozilla.org/security/announce/2012/mfsa2012-67.html
http://www.mozilla.org/security/announce/2012/mfsa2012-68.html
http://www.mozilla.org/security/announce/2012/mfsa2012-69.html
http://www.mozilla.org/security/announce/2012/mfsa2012-70.html
http://www.mozilla.org/security/announce/2012/mfsa2012-71.html
http://www.mozilla.org/security/announce/2012/mfsa2012-72.html

SecurityFocus:

http://www.securityfocus.com/bid/55249
http://www.securityfocus.com/bid/55257

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1956
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1970
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1971
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1972
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1973
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1974
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1975
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1976
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3956
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3957

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3958
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3959
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3960
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3961
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3962
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3963
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3964
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3965
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3966
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3967
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3968
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3969
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3970
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3971
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3972
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3973
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3975
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3978
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3979
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3980